Seguridad INFORMÁTICA: protección de activos LÓGICOS

La seguridad en sistemas de información dispone de métodos y técnicas para poder abordar los diferentes problemas, ya sea para garantizar la continuidad del negocio o para proteger la información, haciendo que ésta sea accesible únicamente para los usuarios adecuados. En cualquier caso, es imprescindible realizar inversiones en esta área antes de tener dificultades que se traduzcan en grandes costes para las organizaciones

Enrique Antón Peregrina

Gerente Soluciones Tecnológicas de Burke

Ficha Técnica

Autor: Enrique Antón Peregrina

Título: Seguridad informática: protección de activos lógicos

Fuente: Estrategia Financiera, nº 216. Abril 2005

Localizador: 36 / 2005

Resumen: Uno de los activos mas importantes de una organización es su conocimiento del negocio acumulado a lo largo de los años y bajo diversos entornos económicos. Pero este conocimiento o cúmulo de información y datos empresariales puede muchas veces verse amenazado por riesgos imprevisibles o simplemente por la propia manipulación del personal de la compañía.

Por eso, las empresas deben ser capaces de implementar sistemas que les permitan tener dicha información accesible pero protegida de cualquier ataque, tanto externo como interno. Mecanismos de seguridad como los sistemas de encriptación garantizan esa protección de la información y la propia continuidad del negocio.

Descriptores: Planificación estratégica, seguridad informática, sistemas de información, gestión de costes, Ley de Protección de Datos, protección perimetral, conocimiento del negocio, *firewall*, *hacker*, técnicas de encriptación.

Todas las inversiones realizadas en sistemas de información no valen para nada; toda la tecnología desarrollada para soportar los sistemas de información no vale para nada; todo el esfuerzo realizado por el personal de sistemas de información no vale para nada; Nada de esto merece la pena si los sistemas de información no están disponibles en el momento en que se necesitan para las tomas de decisiones.

Cada vez que tratamos de incidir en temas de seguridad y, en particular, de seguridad informática, tenemos la sensación de poder llegar a imaginar tanto el problema como las soluciones.

Trataremos de descubrir brevemente aspectos que merecen algunas reflexiones por la trascendencia que pueden llegar a tener.

No cabe duda de que uno de los activos mas importantes de una organización es su conocimiento de negocio, acumulado a lo largo de los años de lucha en un sector, con diferentes entornos económicos y con el sello personal de las diferentes personas que la han dirigido.

Este conocimiento es la base de las diferencias con las otras compañías de la competencia, lo que nos permite mantener nuestra posición en el mercado.

¿DÓNDE RESIDE EL CONOCIMIENTO?

Pero, ¿dónde reside este conocimiento?, ¿está seguro allí?. Tengo que reconocer que no hay una respuesta única a estas preguntas, dado que depende de las políticas de las diferentes compañías, pero, en común, no hay duda de que parte de este conocimiento reside en las personas, parte en los sistemas de información y parte en los papeles que se guardan en algunos despachos.

Como todos sabemos, las personas que ocupamos cierta posición en las compañías manejamos información importante que, a veces, se cataloga como confidencial. Es imposible evitar el conocimiento genérico de esta información, puesto que se necesita para la toma de decisiones, pero también se necesita un conocimiento detallado de una situación, no fácilmente almacenable en nuestra memoria, dado el volumen de información que manejamos. Los sistemas de información nos prestan el servicio de guardarnos esa información, siempre accesible, desde los distintos puntos de vista en que pueden ser analizada.

Si hemos sido capaces de atesorar ese conocimiento de forma que sea accesible por las personas que deben utilizarlo y solamente por ellas, habremos conseguido desarrollar una de las fortalezas de nuestra organización.

UNA AMENAZA

Esta fortaleza ¿se puede convertir en amenaza?. Si no hacemos nada para evitarlo, podemos estar seguros de ello.

En muchas organizaciones, este trabajo no es responsabilidad de nadie, o lo es de quien tiene otras muchas responsabilidades a las que la organización da mucho mas valor, por lo que son prioritarias, y, como los recursos deben ser escasos, ya no queda posibilidad de invertir un minuto en el tema de la seguridad.

No quiero ser derrotista, puesto que conozco a muchos responsables de seguridad informática que velan porque esto no se produzca, aunque he de reconocer que no todas las empresas disponen de objetivos mas amplios de los que marca la Ley de Protección de Datos de Carácter Personal.

Aunque la citada Ley ha ayudado mucho a la concienciación de la necesidad de protección de la información, no hay que auto-engañarse considerando que los activos de la compañía están a salvo desde el momento en que hemos implementado las medidas exigidas para proteger los datos de las personas; estos datos no son necesariamente los que contienen el conocimiento de la organización.

La legislación vigente se preocupa por la defensa de la privacidad pero se sobreentiende que las empresas se preocupan de ellas mismas, en particular de la defensa de sus intereses, como es el del conocimiento adquirido.

Como decía anteriormente, nuestro objetivo fundamental se concreta en que la información de la compañía, en la que seguro se condensa el conocimiento del que hablamos, deberá ser accesible en cualquier momento, desde cualquier lugar, para las personas autorizadas a cada parte de la misma y solamente para ellas:

- En cualquier momento: Si cuando necesitamos acceder a una información para una toma de decisiones, dicha información no es accesible (porque el servidor que la guarda no está disponible, por ejemplo) la decisión tomada pudiera no ser la adecuada.

- Desde cualquier lugar: Si no se puede acceder a la información desde donde me hace falta, mi decisión puede ser equivocada.

Las únicas organizaciones razonablemente protegidas son aquellas que disponen de personal dedicado a la seguridad de los sistemas, con medios para mantener el nivel de seguridad que hayamos decidido

- Para los usuarios autorizados: Si terceros no autorizados también pueden acceder a esta información, se pierde su valor diferencial. La información deja de ser una fortaleza en el momento en que puede ser accedida por cualquiera. (Todos conocen mis cartas).

ACCESO CONFIDENCIAL

Quisiera centrarme en el acceso confidencial a la información. Dado que estoy convencido de que todos quieren conocer mis cartas (les es mas cómodo jugar sabiendo que hago o puedo hacer) debo protegerlas del acceso de los demás.

Para ello, muchas organizaciones afrontan proyectos llamados de Protección Perimetral, que consisten en montar mecanismos que controlen el acceso a los centros físicos o lógicos en los que se encuentran mis servidores, que son los que entiendo contienen el conocimiento de la compañía.

Este es un buen punto de partida, mediante técnicas como las de *firewall* logramos dejar "pasar a los buenos y no pasar a los malos", aunque esto no es fácil de conseguir puesto que termino poniendo mecanismos que hacen difícil el trabajo para todos ("buenos y malos") o dejo agujeros sin cerrar.

Como además los malos son malos pero no tontos, encuentran otros medios para colarse, como puede ser el de engañar a usuarios poco precavidos, gracias a los que nos introducen virus, gusanos, software para espiar, etcétera.

Como también la tecnología ayuda, puesto que encuentran agujeros en numerosos productos instalados en nuestros sistemas de información, o bien forman parte de ellos, desde mecanismos empleados para comunicaciones hasta el producto menos importante, instalado en el ordenador personal de cualquier usuario.

Todos estos agujeros de seguridad son detectados, publicada su existencia así como la forma de emplearlos para asaltar aquellos sistemas que dispongan de los mismos. Lógicamente, los fabricantes llegan a esa información y preparan los parches necesarios para reparar la situación. Estos parches quedan a disposición de los clientes, actualmente en forma de ficheros a los que se puede acceder mediante Internet. También queda clara la forma de instalarlo.

La principal diferencia entre las tácticas de usuarios de sistemas de información y de asaltadores de sistemas está en que los primeros no suelen dar la importancia que tiene a la seguridad de sus sistemas y suele pasar desapercibida la existencia de los agujeros y de los parches para taparlos.

Mientras, los expertos en asaltar sistemas sí almacenan en sus bases de datos la lista de todos los agujeros (con o sin parche), para poder lanzar ataques automáticos buscando cualquier resquicio por donde colarse.

Por cierto, las herramientas necesarias para la realización de estos ataques son públicas: cualquiera que tenga un acceso a Internet puede acceder a estas herramientas.

Por este motivo, la visión de la seguridad en los sistemas de información no debe ser la típica de un proyecto en el que se realizan unas inversiones y hemos resuelto el problema. En el momento en que abordamos el proyecto, estoy seguro de que los mecanismos de protección implementados hacen que nuestro entorno pueda considerarse como razonablemente seguro. Es muy probable que, en un tiempo mínimo, haya aparecido alguna vulnerabilidad de nuestro entorno, que nadie de nuestra organización conoce y lógicamente nadie tiene la obligación de reparar.

Las únicas organizaciones razonablemente protegidas son aquellas que disponen de personal dedicado a la seguridad de los sistemas, con los medios para mantener el nivel de seguridad que hayamos decidido.

Hoy disponemos de servicios de alerta que, para las arquitecturas que tenemos, hacen llegar a diario, al correo electrónico del responsable de Seguridad, la lista de nuevas vulnerabilidades que afectan a sus sistemas, así como las direcciones de las que se pueden bajar los parches.

El coste de estos servicios siempre será muy inferior a los daños producidos por cualquier ataque, aunque solamente se estén empleando nuestros sistemas en forma remota, sin robarnos información alguna. Muchas organizaciones compran anualmente más capacidad de proceso de sus sistemas que será utilizada por quienes la emplean sin su consentimiento, en lugar de ser empleada por sus usuarios.

Cada día aumenta la cantidad de organizaciones que además de disponer de mecanismos de protección perimetral, instalan sondas en sus redes, para analizar posibles conductas sospechosas, tanto por parte de sus usuarios como por parte de terceros, bien mediante software instalado (sin nuestro conocimiento) en nuestros sistemas o bien mediante el acceso a información no autorizada.

Cuando nos enfrentamos a estos temas siempre suele aparecer una pregunta: ¿Por qué a nosotros?

Son varias las respuestas, dependiendo de la imagen de la compañía:

- Aquellas empresas muy conocidas pueden ser blanco de ataques por parte de cualquier *hacker* que pretenda hacerse notar entre su grupo.

- También el espionaje industrial encuentra en los sistemas de información el soporte del conocimiento de la competencia y grandes agujeros para penetrar sin ser vistos, a distancia. Los amigos del espionaje industrial lo tienen ahora mas fácil.

- En cualquier compañía, los propios empleados son los mas interesados en acceder a determinada información, a la que normalmente no tendrían acceso. Todas las compañías buscan personas con experiencia y conocimientos concretos en el sector. En nuestro entorno, es absolutamente frecuente el hecho de que cuando alguien decide un cambio de empresa, se arme de información, antes de pedir la baja en la suya, de forma que cuando llegue a la nueva dispondrá de toda la información a la que tenía acceso además de cualquier otra que pueda conseguir.

Desde dentro, siempre ha sido muy fácil acceder a los sistemas (incluso a aquella información para la que no se está autorizado). El primer objetivo del *hacker* es penetrar a los sistemas. Los usuarios ya están dentro. A veces se les puede abrir una puerta (hay instalaciones en las que cualquier usuario puede instalar un módem, por el que salir al exterior, o dejar entrar a terceros).

ATAQUES DESDE DENTRO

La mayor parte de los ataques contra sistemas de información en una empresa se producen desde dentro. Los empleados descontentos originan grandes perjuicios, puesto que conocen la existencia de la información mas crítica. Los ataques así originados suelen ser muy destructivos. A veces alterando información existente se logran mas perjuicios que haciéndola desaparecer: ¿Quién puede darse cuenta a simple vista de que el importe de una factura ha sido cambiada?, ¿qué ocurriría si no es una sino un grupo numeroso de facturas? y ¿qué pasaría si cambiamos los códigos de cliente?

Por otra parte, hoy empleamos dispositivos con capacidad para almacenar gran cantidad de información, que puede salir de la empresa de forma totalmente inadvertida, sin contar con ordenadores portátiles y PDAs.

Detrás del uso de estos dispositivos están la necesidad y la posibilidad de sacar información de la empresa.

Lógicamente, no podemos poner trabas a la necesidad de emplear la información de la compañía, que está para ser empleada, pero podemos evitar que sea empleada inadecuadamente de manera tan fácil. La modernas técnicas de encriptación permiten hoy cambiar el aspecto de los datos, de manera que solamente puedan ser empleados en determinadas condiciones.

El uso de dispositivos móviles, como ordenadores portátiles o PDAs, debería estar complementado por sistemas de encriptación, que eviten el acceso a la información de terceros que puedan acceder a tales dispositivos.

Para los servidores de la organización, podemos actualmente administrar diferentes perfiles de usuarios, con derechos a acceder a distintas informaciones, de manera que empleando las citadas técnicas de encriptación podemos emplear estrategias de claves de forma que solamente el personal de un departamento puede acceder de forma inteligible a los datos de su departamento.

Muchas organizaciones afrontan proyectos llamados de Protección Perimetral, que consisten en montar mecanismos que controlen el acceso a los centros físicos o lógicos donde se encuentran los servidores

Saltando los mecanismos estándares de protección mediante las herramientas de los sistema operativos podemos acceder a cualquier información de un servidor. Con estas técnicas también accederemos a la citada información, pero será ininteligible. No nos servirá para nada haber saltado las protecciones estándares.

También sería interesante ver la cara de quien haya preparado su salida de la compañía, reforzándose con toda la información interesante, almacenándola poco a poco en casa, en el momento de intentar acceder a la misma. Va a ser imposible, sin el puesto de trabajo de cada día.

De igual forma, quien pretenda acceder a una información encriptada, se llevará la sorpresa de que el acceso será posible pero no podrá entender dicha información; no le valdrá para nada.

Estoy convencido de que merece la pena estudiar la posibilidad de implantar esta tecnología en la empresa. La confidencialidad estará garantizada, al pretender acceder a los datos robados, fuera de la empresa.

EL CORREO ELECTRÓNICO

Quiero aprovechar la oportunidad de hablar sobre la seguridad y la protección del conocimiento para hacer algunas reflexiones acerca de otra herramienta muy empleada: el correo electrónico.

Unos no saben como funciona, otros lo emplean simplemente, pero todos divulgan información que puede llegar a ser confidencial.

Trataré de poner un ejemplo: Ya hace muchos años que se puso de moda enviar una tarjeta postal desde el punto o los puntos donde se pasaban las vacaciones. Esta tarjeta postal, generalmente con una vista interesante del lugar, disponía de un espacio al dorso para poner la dirección postal así como un mensaje para el destinatario.

Lógicamente dicho mensaje era accesible para todo el personal de Correos, por cuyas manos pasaba la tarjeta, así como por el destinatario o sus familiares. No era la mejor forma de enviar mensajes que mantuvieran una cierta privacidad. Para hacer esto, lo mejor era utilizar un sobre, que contenga protegida la información contenida en la carta.

El correo electrónico funciona de una manera parecida, con la diferencia de que de cada mensaje que enviamos y que pasa por varios servidores, en cada uno de ellos deja una copia del mensaje original, que estamos enviando. Estos servidores pueden ser diferentes, dependiendo del camino empleado, dentro de las innumerables posibilidades que proporciona la red, en función del destino. Lo que es común es el servidor desde el que envío mi correo y el que éste emplea en la salida.

Si los mensajes enviados desde mi compañía fueran interesantes para alguien, sería muy fácil tener una buena colección de información que pasar a quien le pueda interesar. Cualquier operador podría obtener unos ingresos extraordinarios absolutamente suculentos.

No es raro encontrar información absolutamente confidencial como anexo a un correo. Posiblemente quien lo envía no sabe el mecanismo anteriormente descrito. Es claro que si lo conociera no enviaría cierta información mediante este procedimiento.

Nuevamente he de incidir en que la tecnología y, en particular, las técnicas de encriptación, nos permiten garantizar la confidencialidad de la información, incluso en estas circunstancias.

Es posible enviar anexionado a un correo electrónico cualquier fichero encriptado, que será desencriptado por el receptor del mismo. Nadie en el camino podrá acceder a esta información.

Cada vez que tratamos de técnicas de encriptación, se puede dar la circunstancia de que intentemos compartir información con personal de la propia organización, autorizado para acceder a dicha información. En este caso las herramientas estándares de la compañía le permitirán acceder sin ningún problema.

En el caso de que el receptor de la información sea de otra organización, lógicamente hay una alternativa a la de instalar un mecanismo de PKI o similar, que también incorpore a cada empresa susceptible de recibir un correo originado en

la nuestra. Hay distintos mecanismos para poder enviar un procedimiento de desencriptado, que se inicia de forma automática una vez que le hemos respondido a una petición de clave, que previamente habremos comunicado al destinatario.

Lo que es claro, es que la información, así enviada, no será accesible a personas situadas en puntos intermedios. Únicamente al destinatario.

VIGILANCIA PERMANENTE

La seguridad en sistemas de información dispone de métodos y técnicas para poder abordar los diferentes problemas, ya sea desde el punto de vista de garantizar la continuidad del negocio (no serán los sistemas de información los que causarían un cese en el mismo) hasta el punto de garantizar la protección de la información, haciendo que la información sea accesible únicamente por los usuarios adecuados.

Los mecanismos de seguridad, en particular los encargados de velar por la protección del conocimiento, deben estar permanentemente al día. Es imprescindible una vigilancia permanente, de modo que las inversiones realizadas sean optimizadas y exprimido el rendimiento que de ellas se puede obtener.

Su uso debe ser habitual, no extraordinario. Debe formar parte de la cultura empresarial, definiendo como parte de las políticas de seguridad de la organización los diferentes niveles de clasificación de la información, así como los niveles de autorización requeridos en cada caso.

Para que se alcancen los objetivos que nos planteamos al definir un proyecto de seguridad, es fundamental la realización periódica de auditorías que verifiquen que los procedimientos empleados se encuentran alineados con los objetivos que se persiguen, identificando, además, posibles agujeros bien de los planes, bien de la implementación de los mismos.

> La información de la compañía deberá estar accesible en cualquier momento, desde cualquier lugar, para las personas autorizadas a cada parte de la misma y sólo para ellas

Un complemento perfecto para estas auditorías lo constituyen los análisis de vulnerabilidad, realizados por los llamados *hackers* éticos y que tratarán de saltarse las defensas, tanto desde Internet, como desde el interior de la compañía. Los posibles agujeros detectados deberán constituir el foco de mejora de nuestra seguridad.

En cualquier caso, debo incidir en que es imprescindible realizar inversiones en este área, antes de tener dificultades que se traducen en grandes costes para las organizaciones. Sería interesante hacer el ejercicio de intentar ponernos en el lugar de ciertas compañías que pueden estar teniendo graves problemas con la forma de continuidad de su negocio, después de los sucesos recientemente acaecidos.

Nuestra organización ¿habría sobrevivido? ▣